V. Summary of Claimed Subject Matter

Claim 1

One or more of the below advantages are achieved by the present claimed subject matter as recited in the media container of independent claim 1 which provides: A secure electronic media container (see at least page 4, lines 7-16, 25-28, and page 6, lines 25-27, and FIG. 2) for storing, transporting and/or providing a rights management interface to electronic media content, said container having said electronic media content (see at least page 4, lines 7-16, page 6, lines 17-19, page 7, lines 1-6, and FIG. 2) stored therein and data (see at least page 4, line 25 to page 5, line 6, page 7, lines 7-14, and FIG. 2), external of but attached to or otherwise associated with said container, representative of the media handler and/or a rights management mechanism required to open and play said content (see at least page 4, line 25 to page 5, line 6, page 7, lines 7-14, and FIG. 2).

A media container embodiment of the claimed subject matter concerns a secure electronic media container for storing, transporting and/or providing a rights management interface to electronic media content. The secure container is "defined broadly in terms of an abstract data container format for containing data." Instant specification at page 4, lines 7-16. The secure container is provided "in the form of a universal 'envelope' or meta-container which allows for arbitrary media formats and arbitrary DRM mechanism." Instant specification at page 4, lines 25-28. In an exemplary embodiment, the container uses a "structured markup syntax such as XML, [and] has at least a <CONTENT> section and a <DRM> section." Instant specification at page 6, lines 25-27 and FIG. 2.

Electronic media content is stored in the container, e.g., an HTML file, a PDF file, an MP3 file, a Word file. Instant specification at page 6, lines 17-19. The stored electronic media content is "encrypted or otherwise arranged within the container having a notional package or 'wrapper' surrounding and protecting the stored data, such that it can only be restructured for use by a specific software program adapted especially for the format in question." Instant specification at page 4, lines 7-16 and FIG. 2. Continuing with reference to the exemplary embodiment description, the "<CONTENT> section specifies the format (e.g. the MIME type) of the content. . . . [and] can either encapsulate the content" or reference the content "by

indirection through a network resource address (e.g. URL or DOI)." Instant specification at page 7, lines 1-6.

Data (also referred to as external data) representative of a media handler and/or a rights management mechanism required to open and play the electronic media content is stored external of but attached to or otherwise associated with the container. The external data is metadata attached or otherwise bound to the secure container containing media content. The metadata is "generally universally readable and/or decipherable and describe[s] the underlying media format and digital rights management mechanism(s) employed to 'package' the content." Instant specification at page 4, line 25 to page 5, line 6 and FIG. 2. A processing application "can evaluate the handling requirements of [the] container, retrieve processing components (if necessary), retrieve and render copyright ownership information, and apply designated copyright management policies." Instant specification at page 4, line 25 to page 5, line 6. Returning again to the exemplary embodiment description, the "<DRM> section specifies the DRM mechanism employed, typically a media-specific encryption mechanism, to package the content . . . [and can] refer to either an installed component on the local system or a distant component or web service." Instant specification at page 7, lines 7-14.

As stated at page 5, lines 1-6 of the instant specification, interoperability is easier to achieve using the present claimed subject matter as "the format of the 'outer' layer of the media container . . . can be standardised, and provide a mechanism whereby a variety of digital rights management (DRM) vendors could create 'plug-in' solutions."

Claim 2

One or more of the below advantages are achieved by the present claimed subject matter as recited in the media container of claim 2 which provides: An apparatus for handling the contents of a secure container as claimed in claim **1**, in which is stored electronic media content of arbitrary format, the apparatus comprising means for determining (see at least page 4, line 25 to page 5, line 6, page 5, lines 25-26, and FIG. 1, element 15 from said external data what, if any, digital rights management mechanism was used to package said content and for retrieving or otherwise accessing an appropriate digital rights management handler (see e.g., at least FIG. 1, element 14 and page 6, lines 1-11) accordingly, means for passing (see at least page 6, lines 1-11

and FIG. 1, elements 14, 15) said content through said digital rights management handler, means for determining (see at least page 5, line 26 to page 6, line 3 and FIG. 1, element 15) from said external data the media handler required to access and handle the content and for retrieving or otherwise accessing an appropriate media handler and means for passing (see at least page 6, lines 1-11 and FIG. 1, elements 14, 15) said content through said media handler (see e.g., at least FIG. 1, element 14 and page 6, lines 1-11).

An apparatus embodiment of the claimed subject matter as claimed in claim 2 concerns an apparatus for handling the contents of a secure container as claimed in claim 1 in which is stored electronic media content of arbitrary format. The apparatus comprises means for determining from external data what, if any, digital rights management mechanism was used to package the content. The means for determining from external data the digital rights management mechanism used corresponds to at least a generic container handler 15 (FIG. 1) which "retrieves details (if any) of the DRM mechanism used to package the data within the secure container 12." Instant specification at page 5, lines 25-26. The data is attached or otherwise bound to the secure container containing media content. The data is "generally universally readable and/or decipherable and describe[s] the underlying media format and digital rights management mechanism(s) employed to 'package' the content." Instant specification at page 4, line 25 to page 5, line 6 and FIG. 2.

The means for determining further comprises retrieving or otherwise accessing an appropriate digital rights management handler accordingly. The means corresponds to at least the generic container handler 15 of FIG. 1 described above. Further, as stated in the instant specification, "[t]he content is first passed through the specified DRM handler 14 and then through the specified media handler, such that the sound recording can now be played by the user and appropriate DRM policies can be applied accordingly." Instant specification at page 6, lines 3-6.

The apparatus comprises means for passing the content through the digital rights management handler as at least the above-described generic container handler 15 (FIG. 1). The digital rights management handler corresponds to at least DRM handler 14 (FIG. 1 and page 6, lines 1-11).

The apparatus comprises means for determining from the external data the media handler required to access and handle the content and for retrieving or otherwise accessing an appropriate media handler for passing the content through the media handler. The means corresponds to at least the generic container handler 15 of FIG. 1 described above. Further, as stated in the instant specification, "details of the media handler required to handle the data, said details being attached to the outer layer of the container 12 as metadata, together with details of how (or where) the required media handler and DRM handler can be obtained (if appropriate)." Instant specification at page 5, line 26 to page 6, line 3. Further still, the "DRM format specification (included in the metadata) indicates how the generic container (or envelope) handler 15 should recognize, reference and/or retrieve (if necessary) the required media handler(s) 16 and, in particular, how to recognise and reference particular DRM handlers or plug-ins. The DRM mechanism may be referenced in a way which is similar to the manner in which MIME types are currently handled." Instant specification at page 6, lines 7-11.

Claim 5

The present claimed subject matter as recited in the media container of dependent claim 5 which provides: A secure electronic container according to claim 3, wherein the metadata (see at least page 5, second full paragraph through page 6, second paragraph, page 6, lines 7-11, page 4, lines 7-16, page 7, lines 1-6, and FIG. 2) describing the underlying media format includes a remote network resource address at which the content itself is stored.

A media container embodiment of the claimed subject matter concerns a secure electronic container for storing, transporting and/or providing a rights management interface to electronic media content. As described above with respect to the media container of independent claim 1, the container has electronic media content stored therein and data, external of but attached to or otherwise associated with the container, representative of a media handler and/or a rights management mechanism required to open and play the content.

The secure container includes media content which has attached or otherwise bound thereto metadata which is universally readable and/or decipherable and describes the underlying media format and digital rights management mechanism(s) employed to package the content. As described above at page 5, second full paragraph through page 6, second paragraph, the electronic media content is stored in the container (Instant specification at page

6, lines 7-11) and is "encrypted or otherwise arranged within the container having a notional package or 'wrapper' surrounding and protecting the stored data (Instant specification at page 4, lines 7-16 and FIG. 2). The "<CONTENT> section specifies the format . . . of the content. . . . [and] can either encapsulate the content" or reference the content "by indirection through a network resource address (e.g., URL or DOI)." Instant specification at page 7, lines 1-6.

The foregoing is achieved by the present claimed subject matter as recited in the media container of dependent claim 5 which provides: A secure electronic container according to claim 3, wherein the metadata (see at least page 5, second full paragraph through page 6, second paragraph, page 6, lines 7-11, page 4, lines 7-16, page 7, lines 1-6, and FIG. 2) describing the underlying media format includes a remote network resource address at which the content itself is stored.

Claim 8

One or more of the below advantages are achieved by the present claimed subject matter as recited in the method of independent claim 8 which provides: A method of handling the contents of a secure container as claimed in claim 1 in which is stored electronic media content of arbitrary format, the method comprising the steps of reading the external data and determining (see at least page 5, line 22 to page 6, line 6) what, if any, digital rights management mechanism was used to package said content, retrieving or otherwise accessing (see at least page 6, lines 3-6, page 7, lines 15-22, and FIG. 2) an appropriate digital rights management handler accordingly, passing (see at least page 6, lines 1-6 and page 6, lines 1-6) said content through said digital rights management handler, reading the external data and determining the media handler required to access and handle the contents, retrieving or otherwise accessing an appropriate media handler, and passing (see at least page 6, lines 1-6 and page 6, lines 1-6) said content through said media handler.

A method embodiment of the claimed subject matter concerns a method of handling the contents of a secure container as claimed in claim 1. The secure container stores electronic media content of arbitrary format as already described above with respect to claim 1. The method includes reading the external data and determining what, if any, digital rights management mechanism was used to package the content. According to an exemplary embodiment, a container handler “retrieves details (if any) of the DRM mechanism used to

package the data within the secure container 12 . . ., said details being attached to the outer layer of the container 12 as metadata." Instant specification at page 5, line 22 to page 6, line 6. The "details of how (or where) the . . . DRM handler can be obtained (if appropriate)" is specified. Instant specification at page 6, lines 2-3. The DRM details specify "how the generic container (or envelope) handler 15 should . . . recognise and reference particular DRM handlers or plug-ins."

The method further includes retrieving or otherwise accessing an appropriate digital rights management handler accordingly and passing the content through the digital rights management handler. "The content is . . . passed through the specified DRM handler 14 . . . and appropriate DRM policies can be applied accordingly." Instant specification at page 6, lines 3-6. When a container handler opens the "outer DRM envelope and determines that a DRM mechanism has been specified, [the handler] knows by the given definition of the DRM format that it must first pass the content through the specified DRM mechanism (like a filter)." Instant specification at page 7, lines 15-22 and FIG. 2.

The method further includes reading the external data and determining the media handler required to access and handle the content and retrieving or otherwise accessing the appropriate media handler and passing the content through the media handler. The metadata of the container (described above) is "readable and/or decipherable and describe[s] the underlying media format . . . so that a processing application (for example, a desktop software tool, web browser, etc.) can evaluate the handling requirements of [the] container, retrieve processing components (if necessary)." Instant specification at page 5, lines 1-6. "[D]etails of the media handler required to handle the data . . . together with details of how (or where) the required media handler . . . can be obtained" are provided in the external data. Instant specification at page 6, lines 1-6.

The present claimed subject matter provides a method of handling the contents of a secure container wherein the container stores and/or transports electronic data and includes data external of the container which is used to specify a wide range of different applications the format of the encapsulated data and provide policies on how to obtain and interpret the data content. Instant specification at page 8, lines 10-14.

Claim 11

One or more of the below advantages are achieved by the present claimed subject matter as recited in the method of independent claim 11 which provides: A method of handling the contents of a secure container as claimed in claim 1 in which is stored electronic media content of arbitrary format, the method comprising the steps of reading the external data and determining (see at least page 5, line 22 to page 6, line 6) what, if any, digital rights management mechanism was used to package said content, retrieving or otherwise accessing (see at least page 6, lines 3-6, page 7, lines 15-22, and FIG. 2) an appropriate digital rights management handler accordingly, passing (see at least page 6, lines 1-6 and page 6, lines 1-6) said content through said digital rights management handler, reading the external data and determining (see at least page 5, line 22 to page 6, line 6) the media handler required to access and handle the contents, retrieving or otherwise accessing the determined media handler, and passing (see at least page 6, lines 1-6 and page 6, lines 1-6) said content through said media handler.

A method embodiment of the claimed subject matter concerns a method of handling the contents of a secure container as claimed in claim 1. The secure container stores electronic media content of arbitrary format as already described above with respect to claim 1. The method includes reading the external data and determining what, if any, digital rights management mechanism was used to package the content. According to an exemplary embodiment, a container handler "retrieves details (if any) of the DRM mechanism used to package the data within the secure container 12 . . ., said details being attached to the outer layer of the container 12 as metadata." Instant specification at page 5, line 22 to page 6, line 6. The "details of how (or where) the . . . DRM handler can be obtained (if appropriate)" is specified. Instant specification at page 6, lines 2-3. The DRM details specify "how the generic container (or envelope) handler 15 should . . . recognise and reference particular DRM handlers or plug-ins."

The method further includes retrieving or otherwise accessing an appropriate digital rights management handler accordingly and passing the content through the digital rights management handler. "The content is . . . passed through the specified DRM handler 14 . . . and appropriate DRM policies can be applied accordingly." Instant specification at page 6, lines 3-6. When a container handler opens the "outer DRM envelope and determines that a

DRM mechanism has been specified, [the handler] knows by the given definition of the DRM format that it must first pass the content through the specified DRM mechanism (like a filter)." Instant specification at page 7, lines 15-22 and FIG. 2.

The method further includes reading the external data and determining the media handler required to access and handle the content and retrieving or otherwise accessing the determined media handler and passing the content through the media handler. The metadata of the container (described above) is "readable and/or decipherable and describe[s] the underlying media format . . . so that a processing application (for example, a desktop software tool, web browser, etc.) can evaluate the handling requirements of [the] container, retrieve processing components (if necessary)." Instant specification at page 5, lines 1-6. "[D]etails of the media handler required to handle the data . . . together with details of how (or where) the required media handler . . . can be obtained" are provided in the external data. Instant specification at page 6, lines 1-6.

The present claimed subject matter provides a method of handling the contents of a secure container wherein the container stores and/or transports electronic data and includes data external of the container which is used to specify a wide range of different applications the format of the encapsulated data and provide policies on how to obtain and interpret the data content. Instant specification at page 8, lines 10-14.

Claim 10

One or more of the below advantages are achieved by the present claimed subject matter as recited in the apparatus of independent claim 10 which provides: Apparatus for handling the contents of a secure container as claimed in claim **1**, in which is stored electronic media content of arbitrary format, the apparatus comprising a processor arrangement for (a) determining (see at least page 5, line 22 to page 6, line 6) from said external data what, if any, digital rights management mechanism was used to package said content and for retrieving or otherwise accessing (see at least page 6, lines 3-6, page 7, lines 15-22, and FIG. 2) an appropriate digital rights management handler accordingly; (b) passing (see at least page 6, lines 1-6 and page 6, lines 1-6) said content through said digital rights management handler; and (c) determining (see at least page 5, line 22 to page 6, line 6) from said external data the media handler required to

access and handle the content and for retrieving or otherwise accessing an appropriate media handler.

An apparatus embodiment of the claimed subject matter concerns an apparatus for handling the contents of a secure container as claimed in claim 1. The apparatus comprises a processor arrangement for performing steps similar to those described above with respect to claim 11.